CONVOCATION FIGHT FOR THE FUTURE

Financial Confidentiality in the Age of Digital Surveillance:

An Audit of Current Privacy Technologies Available to Mutual Aid Organizations
Created for Fight for the Future by Convocation Research+Design

Abstract

In an era where digital surveillance is pervasive and financial transactions are increasingly conducted online, maintaining privacy has become a paramount concern to mutual aid organizations such as abortion funds, disaster relief funds, gender-affirming care funds, and bail funds—as well as individuals who receive their support. This report, "Financial Privacy in the Age of Digital Surveillance: An Audit of Current Privacy Technologies Available to Mutual Aid Organizations,"commissioned by Fight for the Future and conducted by Convocation Research + Design, explores the effectiveness of various privacy technologies in safeguarding financial data through the process of transferring from entity to individual.

Through a comprehensive audit, we evaluate the strengths and weaknesses of current privacy tools and protocols, such as cryptocurrencies, anonymizing services, and conventional financial services. Our analysis highlights the potential of these technologies to protect users' financial confidentiality against unauthorized access and data breaches, while also addressing the challenges posed by regulatory scrutiny and the evolving landscape of digital surveillance. The findings underscore the importance of robust privacy measures and informed policy-making to ensure financial security and individual autonomy in the digital age. This report aims to provide stakeholders with actionable insights into the state of financial privacy technologies and recommendations for enhancing their adoption and efficacy.

Table of Contents

Overall Findings

After extensive research, we have concluded that all cryptocurrencies considered in this report would meet or exceed reasonable protections for privacy and security concerns for financial transactions between individuals and mutual aid groups, except for Bitcoin. We think that Monero, MobileCoin, and ZCash (when in private mode) are all great options for secure and

confidential transactions, but with Bitcoin's attention from law enforcement and recent news of trackability we can't currently recommend it for use in mutual aid funds. As for non-crypto options, we have concluded the most secure option is USPS Money Order, which is essentially cash; with Apple Tap to Cash coming in second, with some caveats. As you'll find in the report, the best choice really depends on the individual's own personal threat model and the technical capacity of the mutual aid organization as to which financial tool is best for them.

Key Findings on Emerging Technologies

- Bitcoin's Privacy Limitations: While Bitcoin provides pseudonymity, transactions are traceable on the public blockchain, making it possible to link addresses to real-world identities under certain conditions.
- Monero, Zcash, and MobileCoin's Strong Privacy Features: these cryptocurrencies offer enhanced privacy through features like ring signatures, stealth addresses, and confidential transactions, making it significantly more challenging for law enforcement to trace transactions compared to Bitcoin.
- Regulatory Challenges: Privacy-focused cryptocurrencies like Monero, MobileCoin, and Zcash face increased regulatory scrutiny and potential restrictions due to their association with illicit activities and difficulty in tracking.
- Law Enforcement Techniques: Various techniques are used to trace cryptocurrency transactions, including blockchain analysis, clustering, intelligence gathering, and cooperation with exchanges, but the effectiveness varies based on the cryptocurrency's privacy features.
- Privacy vs. Usability Trade-offs: Cryptocurrencies that offer strong privacy protections, such as Monero and MobileCoin, often face challenges with user adoption, complexity, and regulatory hurdles, which impact their overall usability and acceptance.

Terminology

- Privacy: the state or condition of being free from being observed or disturbed by other people or the state of being free from public attention.
- Anonymity: a situation in which a person is not known by or spoken of by name.
- Pseudonymity: a state of operating under a fictitious name, used especially by an author to conceal their identity; pen name. The use of a different name from your real name, especially on something you have written: Much of the web is dominated by anonymity and pseudonymity.
- Threat Model: the process of using hypothetical scenarios, system diagrams, and testing to help secure information or data. By identifying vulnerabilities, helping with risk assessment, and suggesting corrective action, threat modeling helps improve cybersecurity and trust in key systems.

- Cryptocurrency: a digital or virtual form of currency that relies on cryptographic principles for security. It operates on decentralized networks using blockchain technology, enabling peer-to-peer transactions without the need for intermediaries. Cryptocurrencies are characterized by their digital nature, cryptographic security, and potential for varying levels of user anonymity and privacy.
- Crypto Address: a crypto address is a unique identifier, composed by a string of letters and numbers, that serves as a virtual location to where a cryptocurrency can be sent. You can see it as being your email address, but in the crypto ecosystem.
- Crypto Wallet: a crypto wallet is a digital tool that allows users to store, manage, and interact with their cryptocurrencies. Crypto wallets are designed to store your private key, keeping your crypto accessible at all times. They also allow you to send, receive, and spend cryptocurrencies like Bitcoin. Key components of a wallet:
    - Public Key: A public key is like an account number. It is used to receive cryptocurrencies and can be shared with others.
    - Private Key: A private key is like a password. It is used to sign transactions and access your cryptocurrency holdings. It must be kept secure and private.
    - Address: A crypto wallet address is a hashed version of the public key. It is a string of characters used to send and receive cryptocurrencies.
- Know Your Customer (KYC): Know Your Customer, is a legal requirement for centralized exchanges to verify the identities of their users. It aims to prevent the use of cryptocurrencies for money laundering, tax evasion, and financing illegal activities.
- Blockchain: A blockchain is a distributed database that continuously grows with a record of all of the transactions that have occurred with a given cryptocurrency.
- Fungibility: Property of a currency whereby two units can be substituted in place of one another. Fungibility means that two units of a currency can be mutually substituted and the substituted currency is equal to another unit of the same size.

Threat Modeling

Threat Modeling is a systematic process used to identify, assess, and address potential security threats that could compromise the integrity, confidentiality, and availability of systems, particularly in the realm of cybersecurity. The process involves anticipating potential threats, understanding the assets that need protection, evaluating the impact of those threats, and designing security measures to mitigate them. By simulating different attack scenarios and understanding how different vulnerabilities can be exploited, organizations can create more robust security frameworks to protect their assets.

When it comes to financial transactions, especially those involving sensitive payments for mutual aid, privacy and confidentiality are paramount. Mutual aid often involves communities pooling resources to support each other, sometimes in vulnerable situations where individuals' privacy is crucial. Threat modeling becomes critical here as it helps identify potential risks that could expose financial details or the identities of those involved in these transactions. This is particularly important because mutual aid often operates outside traditional financial systems, which may lack the same level of built-in security and oversight.

By engaging in threat modeling, mutual aid organizers can anticipate risks such as data breaches, unauthorized access, or tracking of transactions that could endanger participants. For example, understanding how financial data might be intercepted during a transfer can lead to the adoption of encryption or anonymization techniques. It can also help in selecting secure payment platforms that prioritize user privacy and offer robust security features. Ultimately, threat modeling is not just about identifying vulnerabilities, but also about building trust within the community by ensuring that financial support remains confidential and secure.

This approach is essential not only for protecting individual privacy but also for maintaining the integrity of the mutual aid system as a whole, ensuring that it remains a safe and effective means of community support.

Detailed Analysis on Individual Methods aka Cryptocurrency Analysis

To perform a comparative analysis of Bitcoin, Monero, MobileCoin, and Zcash, let's explore their key characteristics, use cases, privacy features, consensus mechanisms, and community support. Each of these cryptocurrencies has unique properties that cater to different user needs and preferences.

Comparative Summary

Feature	Bitcoin (BTC)	Monero (XMR)	MobileCoin (MOB)	Zcash (ZEC)
Launch Year	2009	2014	2020	2016
Primary Use Case	Digital currency	Privacy-focused currency	Mobile privacy transactions	Optional privacy currency
Blockchain Type	Public	Public, privacy-enhanced	Permissioned	Public, optional privacy
Consensus Mechanism	Proof of Work (PoW)	Proof of Work (PoW) with RandomX	Federated Byzantine Agreement	Proof of Work (PoW)

Privacy Features	Limited	Strong (RingCT, stealth addresses)	Strong (CryptoNote, Intel SGX)	Strong (zk-SNARKs)
Block Time	~10 minutes	~2 minutes	Very fast	~75 seconds
Adoption and Liquidity	High	Moderate	Low	Moderate
Regulatory Scrutiny	Moderate	High	Moderate	High

Each cryptocurrency has its strengths and weaknesses, catering to different user needs ranging from privacy, scalability, to usability in mobile environments. The choice between them depends on the specific requirements of the user and their tolerance for risk, privacy needs, and regulatory environment.

Bitcoin

Bitcoin is a decentralized digital currency created in 2008 by an anonymous person or group known as Satoshi Nakamoto. It operates on a peer-to-peer network, allowing users to send and receive payments without relying on a central authority like a bank. Bitcoin transactions are recorded on a public ledger called the blockchain, which ensures transparency and security. While Bitcoin is often referred to as "digital gold" due to its fixed supply and potential for long-term value storage, it is also used as a medium of exchange. Its pseudonymous nature offers limited privacy, and its high market capitalization and widespread adoption make it the most recognized and valuable cryptocurrency in the world.

Pros of Bitcoin for Privacy and Security

1. Pseudonymity:
    - Bitcoin transactions do not require personal information, only wallet addresses, which are pseudonymous. This provides a layer of privacy as the real-world identity of a wallet holder is not inherently linked to their transactions.
2. Decentralization:
    - The decentralized nature of Bitcoin means there is no central authority or single point of failure that can be compromised. This reduces the risk of censorship and centralized data breaches.
3. Encryption:
    - Bitcoin transactions are secured by strong cryptographic algorithms, making it extremely difficult for unauthorized parties to alter transaction data.
4. Transparency:

- The Bitcoin blockchain is a public ledger, which can enhance security by allowing anyone to verify transactions. This transparency can help in identifying and mitigating fraudulent activities.

5. Control Over Funds:
    - Bitcoin users have full control over their funds, without reliance on intermediaries like banks, which can be a security advantage as it eliminates the risk of bank failures or freezes.

Cons of Bitcoin for Privacy and Security

1. Pseudonymity Limitations:
    - While Bitcoin addresses are pseudonymous, transactions can be traced on the public ledger. If an address is ever linked to an individual, all associated transactions can be identified.
2. Regulatory Scrutiny:
    - Governments and regulatory bodies are increasingly focusing on Bitcoin transactions to prevent illegal activities such as money laundering and tax evasion. This can lead to increased surveillance and reduced privacy.
3. Lack of Reversibility:
    - Bitcoin transactions are irreversible, which means if funds are sent to the wrong address or stolen, they cannot be recovered. This lack of recourse can be a significant security risk.
4. Potential for Hacks and Scams:
    - While the Bitcoin protocol itself is secure, the surrounding ecosystem, including exchanges, wallets, and other services, is susceptible to hacks, phishing attacks, and scams. Users must be vigilant in securing their private keys and using reputable services.
5. User Responsibility:
    - The security of Bitcoin largely depends on the user's ability to safeguard their private keys and use best practices for cybersecurity. If private keys are lost or stolen, the associated Bitcoin is irrecoverable.
6. Scalability issues:
    - This results in slower transaction times and higher fees during peak usage.
7. Network Privacy Limitations:
    - While all cryptocurrencies offer strong on-chain privacy, it does not inherently protect against network-level privacy threats, such as IP address tracking during transactions. Users may need to employ additional privacy tools (like Tor) to enhance their overall privacy when using any cryptocurrency.

Blockchain Analysis

1. Transaction Tracing:

- Bitcoin transactions are recorded on the blockchain, a public ledger that anyone can access. Law enforcement agencies use blockchain analysis tools to trace the flow of Bitcoin from one address to another.

2. Cluster Analysis:
   - Agencies group Bitcoin addresses that appear to be controlled by the same entity, known as clustering. This helps in identifying patterns and connections between different addresses.
3. Heuristic Methods:
   - Various heuristics, such as common input ownership (multiple inputs in a transaction often belong to the same entity) and change address detection (identifying the address where leftover Bitcoin from a transaction is sent), are used to link addresses.

Cooperation with Exchanges and Wallet Providers

1. KYC/AML Compliance:
   - Many Bitcoin exchanges and wallet providers are required to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. They collect personal information from users, which law enforcement can request during investigations.
2. Subpoenas and Legal Requests:
   - Law enforcement can issue subpoenas or other legal requests to exchanges and wallet providers to obtain user information linked to specific Bitcoin addresses.

Intelligence and Surveillance

1. Network Monitoring:
   - By monitoring Bitcoin network traffic, law enforcement can gather information on the IP addresses of nodes broadcasting transactions. This can help in identifying the geographical location of users.
2. Undercover Operations:
   - Law enforcement may conduct undercover operations, such as posing as buyers or sellers on darknet markets, to gather information on Bitcoin transactions and the individuals behind them.

Collaboration with Blockchain Analysis Firms

1. Third-Party Services:
   - Agencies often collaborate with specialized blockchain analysis firms that provide sophisticated tools and expertise for tracking Bitcoin transactions. Companies like Chainalysis, Elliptic, and CipherTrace are examples of such firms.

Using Advanced Techniques

- Deanonymization Techniques:
    - Law enforcement uses various deanonymization techniques to link Bitcoin addresses to real-world identities. This can involve analyzing patterns of transactions, correlating blockchain data with off-chain information, and exploiting weaknesses in the way some users handle their Bitcoin.
- Machine Learning and AI:
    - Advanced machine learning and artificial intelligence algorithms are employed to detect suspicious patterns and behaviors in Bitcoin transactions.

Bitcoin offers significant advantages for privacy and security through its pseudonymous nature, decentralized structure, and strong cryptographic foundations. However, it also presents challenges, including traceability on the public ledger, regulatory scrutiny, irreversibility of transactions, and the necessity for robust personal security practices. Users need to be well-informed and proactive in managing their Bitcoin securely.

Monero

Monero (XMR) is a privacy-focused cryptocurrency designed to provide enhanced anonymity and untraceability for its users. This makes it more challenging for law enforcement to track compared to Bitcoin. However, there are still some methods and strategies that law enforcement can employ to investigate activities involving Monero:

Pros of Monero for Privacy and Security

1. Strong Privacy Features:
    - Ring Signatures: These obscure the sender's address by mixing it with a group of others, making it difficult to determine the actual sender.
    - Stealth Addresses: These ensure the recipient's address is not publicly linked to their transactions by generating a unique one-time address for each transaction.
    - Confidential Transactions (RingCT): These hide the transaction amount, making it difficult to determine the value of any given transaction.
2. Decentralization:
    - Like other cryptocurrencies, Monero is decentralized, reducing the risk of central authority control or a single point of failure that could be exploited.
3. Fungibility:
    - Every Monero coin is indistinguishable from another, which enhances privacy by preventing coins from being blacklisted or traced back to previous transactions.
4. Active Development and Community:
    - Monero has a strong, active development team continuously working on improving its privacy features and security, as well as a supportive community advocating for privacy.
5. Encrypted Memo Fields:

- Monero allows users to add encrypted messages to transactions, ensuring that any additional information shared remains private.

Cons of Monero for Privacy and Security

1. Regulatory Scrutiny:
   - Monero's strong privacy features attract regulatory scrutiny as they can be used for illicit activities, leading to potential restrictions or bans by governments.
2. Limited Adoption:
   - Due to regulatory concerns and the complexity of its privacy features, Monero has limited adoption compared to more mainstream cryptocurrencies like Bitcoin.
3. Complexity:
   - The advanced privacy features of Monero can be complex for users to understand and properly implement, potentially leading to mistakes that could compromise privacy.
4. Exchange Limitations:
   - Many cryptocurrency exchanges are hesitant to list Monero due to its association with illicit activities and regulatory risks, limiting its liquidity and ease of exchange.
5. Potential for User Error:
   - As with all cryptocurrencies, if users do not properly secure their private keys or use best practices for digital security, their Monero can be stolen, and there is no recourse for recovering lost funds.
6. Network Privacy Limitations:
   - While all cryptocurrencies offer strong on-chain privacy, it does not inherently protect against network-level privacy threats, such as IP address tracking during transactions. Users may need to employ additional privacy tools (like Tor) to enhance their overall privacy when using any cryptocurrency.

Techniques Used by Law Enforcement to Track Monero

1. Blockchain Analysis Limitations:
   - Unlike Bitcoin, Monero transactions use ring signatures, stealth addresses, and confidential transactions to obfuscate transaction details. This makes traditional blockchain analysis tools much less effective.
2. Intelligence and Human Resources:
   - Law enforcement may rely on intelligence gathering and human resources to track down Monero users. This can include undercover operations, informants, and surveillance to gather information on suspects involved in illegal activities.
3. Network Monitoring:

- Monitoring the Monero network traffic can provide some insights, such as IP addresses of nodes participating in transactions. However, Monero's use of Dandelion++ for transaction propagation helps to protect user privacy by making it harder to trace the origin of transactions.

4. Exchange Cooperation:
    - Law enforcement can target exchanges where Monero is converted into fiat currency or other cryptocurrencies. Exchanges that comply with KYC and AML regulations can provide user information upon legal request. Tracking the movement of funds through exchanges can help identify individuals involved.
5. Targeting Weak Links:
    - Law enforcement can focus on vulnerabilities in the overall ecosystem rather than the Monero protocol itself. For instance, they might look for weak links in user behavior, such as poor operational security (OPSEC) practices, that can expose identities.
6. De-anonymization Attacks:
    - Advanced de-anonymization techniques, although limited, can sometimes be applied. For example, statistical analysis of transaction patterns, timing analysis, and other heuristics might be used to link transactions over time.
7. Collaboration with Blockchain Analysis Firms:
    - Some blockchain analysis firms are developing tools to analyze privacy coins, including Monero. While these tools are not as advanced as those for Bitcoin, they can still provide some insights into Monero transactions.
8. Legal Pressure on Service Providers:
    - Law enforcement can exert legal pressure on service providers that accept Monero, such as online marketplaces or payment processors, to gather information on transactions and users.
9. Open-Source Intelligence (OSINT):
    - Investigators can use OSINT techniques to gather information from publicly available sources, such as forums, social media, and other online platforms where individuals may discuss or advertise their use of Monero. An example of this would be to look specifically for people listing their Monero addresses or advertising they use Monero online on social media, forums, etc.
10. Collaborating with International Agencies:
    - International cooperation can be crucial in tracking Monero transactions, especially when they cross borders. Law enforcement agencies around the world share information and resources to combat the use of Monero in illegal activities.

Challenges in Tracking Monero

1. Enhanced Privacy Features:

- Monero's privacy features, including ring signatures, stealth addresses, and confidential transactions, make it difficult to link transactions to individuals or to trace the flow of funds.

2. Lack of Public Ledger Transparency:
   - The obfuscation techniques used in Monero transactions result in a lack of transparency on the public ledger, limiting the effectiveness of traditional blockchain analysis.
3. Evolving Privacy Techniques:
   - As Monero continues to evolve, its privacy techniques are continuously improved, making it increasingly challenging for law enforcement to develop effective tracking methods.

While Monero's advanced privacy features present significant challenges for law enforcement, a combination of traditional investigative techniques, cooperation with exchanges and service providers, network monitoring, and advanced analysis methods can still provide some avenues for tracking and identifying individuals involved in activities using Monero. However, the effectiveness of these methods is generally more limited compared to tracking Bitcoin or other cryptocurrencies with less emphasis on privacy. Monero offers significant privacy and security advantages through its robust privacy features, decentralization, and fungibility. However, these same features also lead to regulatory challenges, limited adoption, and potential complexities for users. Those prioritizing privacy may find Monero highly beneficial, but they must also be aware of the associated risks and regulatory landscape.

MobileCoin

MobileCoin (MOB) is a privacy-focused cryptocurrency designed for fast, secure, and private transactions, often used in mobile applications. Tracking MobileCoin poses significant challenges for law enforcement due to its privacy features. However, there are still strategies that can be employed:

Pros of MobileCoin for Privacy and Security

1. Strong Privacy Features:
   - Confidential Transactions: MobileCoin uses Ring Confidential Transactions (RingCT) to conceal transaction amounts and make transactions more private.
   - Secure Messaging Integration: MobileCoin is integrated with messaging apps like Signal, which allows for secure and private transactions within a familiar and secure platform.
2. Ease of Use:
   - MobileCoin is designed to be user-friendly, with a focus on seamless integration into mobile applications. This makes it more accessible to non-technical users who prioritize privacy.

3. High Transaction Speed:
    - MobileCoin aims to offer fast transaction times, which enhances security by reducing the time window for potential attacks on the network.
4. Environmentally Friendly:
    - MobileCoin uses the Stellar Consensus Protocol (SCP) for its consensus mechanism, which is more energy-efficient compared to traditional proof-of-work cryptocurrencies like Bitcoin.
5. Decentralization:
    - As with other cryptocurrencies, MobileCoin is decentralized, reducing the risk of central authority control or a single point of failure that could be exploited.

Cons of MobileCoin for Privacy and Security

1. Regulatory Scrutiny:
    - Like other privacy-focused cryptocurrencies, MobileCoin could attract regulatory scrutiny due to its potential use in illicit activities. This can lead to potential restrictions or bans in certain jurisdictions.
2. Limited Adoption:
    - Due to regulatory concerns and competition from other established cryptocurrencies, MobileCoin has limited adoption and acceptance compared to more mainstream options like Bitcoin and Ethereum.
3. Dependence on Mobile Platforms:
    - MobileCoin's integration with mobile messaging apps is a double-edged sword. While it enhances usability, it also makes users dependent on the security of the underlying mobile platforms and apps.
4. Exchange Limitations:
    - Privacy-focused cryptocurrencies often face limitations in being listed on major exchanges due to regulatory compliance concerns. This can affect MobileCoin's liquidity and ease of exchange.
5. Potential for User Error:
    - As with all cryptocurrencies, if users do not properly secure their private keys or follow best practices for digital security, their MobileCoin can be stolen. The integration with mobile apps might also introduce new vectors for user error or security breaches.
6. Network Privacy Limitations:
    - While all cryptocurrencies offer strong on-chain privacy, it does not inherently protect against network-level privacy threats, such as IP address tracking during transactions. Users may need to employ additional privacy tools (like Tor) to enhance their overall privacy when using any cryptocurrency.

Techniques Used by Law Enforcement to Track MobileCoin

1. Blockchain Analysis:
    - MobileCoin transactions are encrypted and designed to be private, similar to Monero. This limits the effectiveness of traditional blockchain analysis tools. However, if any vulnerabilities or weaknesses in the encryption methods are discovered, it could provide a way to analyze transaction data.
2. Intelligence Gathering:
    - Law enforcement can rely on intelligence gathering, including undercover operations, informants, and surveillance, to gather information on suspects involved in illegal activities using MobileCoin.
3. Network Monitoring:
    - Monitoring the MobileCoin network traffic can provide some insights, such as IP addresses of nodes participating in transactions. This can help in identifying the geographical locations of users.
4. Exchange Cooperation:
    - Law enforcement can target exchanges where MobileCoin is converted into fiat currency or other cryptocurrencies. Exchanges that comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations can provide user information upon legal request. Tracking the movement of funds through exchanges can help identify individuals involved.
5. Targeting Weak Links:
    - Law enforcement can focus on vulnerabilities in the overall ecosystem rather than the MobileCoin protocol itself. This includes looking for weak links in user behavior, such as poor operational security (OPSEC) practices, that can expose identities.
6. De-anonymization Attacks:
    - Advanced de-anonymization techniques, although limited, can sometimes be applied. For example, statistical analysis of transaction patterns, timing analysis, and other heuristics might be used to link transactions over time.
7. Collaboration with Blockchain Analysis Firms:
    - Some blockchain analysis firms are developing tools to analyze privacy coins, including MobileCoin. While these tools are not as advanced as those for Bitcoin, they can still provide some insights into MobileCoin transactions.
8. Legal Pressure on Service Providers:
    - Law enforcement can exert legal pressure on service providers that accept MobileCoin, such as online marketplaces or payment processors, to gather information on transactions and users.
9. Open-Source Intelligence (OSINT):
    - Investigators can use OSINT techniques to gather information from publicly available sources, such as forums, social media, and other online platforms where individuals may discuss or advertise their use of MobileCoin.
10. Collaborating with International Agencies:

- International cooperation can be crucial in tracking MobileCoin transactions, especially when they cross borders. Law enforcement agencies around the world share information and resources to combat the use of MobileCoin in illegal activities.

Challenges in Tracking MobileCoin

1. Enhanced Privacy Features:
   - MobileCoin's privacy features, including encrypted transactions on the Signal and Sentz apps, make it difficult to link transactions to individuals or trace the flow of funds.
2. Lack of Public Ledger Transparency:
   - The obfuscation techniques used in MobileCoin transactions result in a lack of transparency on the public ledger, limiting the effectiveness of traditional blockchain analysis.
3. Evolving Privacy Techniques:
   - As MobileCoin continues to evolve, its privacy techniques are continuously improved, making it increasingly challenging for law enforcement to develop effective tracking methods.

Tracking MobileCoin is challenging for law enforcement due to its strong privacy features. While traditional blockchain analysis methods are less effective, a combination of intelligence gathering, cooperation with exchanges, network monitoring, targeting weak links, and using advanced de-anonymization techniques can still provide some avenues for investigation. However, the effectiveness of these methods is generally limited compared to cryptocurrencies with less emphasis on privacy. MobileCoin offers significant privacy and security benefits, particularly through its integration with secure messaging platforms, ease of use, and strong privacy features like RingCT. However, it also faces challenges such as regulatory scrutiny, limited adoption, and potential vulnerabilities associated with its dependence on mobile platforms. Users who prioritize privacy and seek an easy-to-use mobile cryptocurrency may find MobileCoin appealing, but they must also be aware of the associated risks and regulatory landscape.

Sentz App:

The Sentz App is a payment platform tailored for freelancers and creators, allowing them to quickly invoice clients and receive payments in stablecoins, particularly eUSD. This digital currency, pegged to the US dollar, can be held in the app's wallet or converted to local currency when withdrawn to a bank. Available in over 180 countries, Sentz offers end-to-end encryption for secure, peer-to-peer payments. Users can sign up with just a phone number and email and can send invoices or payment requests via personalized links.

Sentz is designed for fast transactions with minimal fees, even for international transfers, which makes it popular among remote workers. It allows various funding methods, including credit cards and stablecoins, and enables users to back up account access securely with a PIN and a 24-word secret phrase. The app is particularly well suited for those needing quick international payments without relying on traditional banking networks.

1. Does Sentz break the direct link between sender and recipient?

- Direct Links: Sentz shares user information (e.g., public wallet addresses and avatars) with recipients if you connect with another user. This means the service does not inherently anonymize or obfuscate the transaction trail between sender and recipient.
- Transaction and Payment Information: Sentz collects and processes transactional data to facilitate payments. If Sentz does not explicitly employ privacy-preserving techniques (e.g., mixing services, pseudonymous wallet systems, or cryptographic measures), then it likely maintains a traceable connection between the two parties.
  Conclusion: Sentz does not explicitly state that it breaks the link between sender and recipient. The transaction details might be accessible to Sentz or potentially available to third parties in compliance with legal requests.

2. Does Sentz collect IP addresses of senders and recipients?

Yes, Sentz collects and stores IP addresses as part of its Internet Activity and Usage Data policies. This includes the IP address of devices interacting with the service and geolocation data (including precise location, if enabled). IP addresses can be used to infer the physical location of users and potentially identify them.

3. Implications for Users Seeking Privacy

- Privacy Risks: Given that Sentz collects extensive user data (IP addresses, device identifiers, geolocation, and transactional information), there are potential risks if this data is subpoenaed or accessed by third parties.
- Data Sharing: Sentz shares information for legal compliance, fraud prevention, and with business partners, which could expose sensitive details about the nature of transactions and parties involved.
- Public Wallet Addresses: Sharing a public wallet address with recipients also introduces traceability since blockchain transactions (if applicable) can often be tracked.

Recommendations:

If the intent is to protect the anonymity of abortion funds, recipients, or any high-risk entity, Sentz may not provide adequate safeguards given its data collection and sharing practices. Instead, consider alternatives designed for privacy:

- Privacy-Enhanced Payment Platforms: Explore platforms explicitly designed for anonymity (e.g., Monero for cryptocurrencies or privacy-centric donation systems).
- Use of VPNs or Tor: If continuing to use Sentz, employ tools like VPNs or Tor to mask IP addresses.

For practical limitations, some users report challenges with funding and withdrawing funds seamlessly, especially for those unfamiliar with cryptocurrency exchanges. The platform's stability and availability may vary, depending on regional partnerships and app maintenance. However, Sentz is working on making the app more user-friendly by streamlining these processes, aiming to appeal to a broader user base by partnering with traditional banking channels for smoother transitions between fiat and crypto.

Law enforcement can potentially track transactions or obtain user data on the Sentz app by utilizing a few key methods, depending on the level of cooperation with MobileCoin, the company behind Sentz, and the regulatory frameworks of the involved countries. Here are some common approaches:

1. Account Verification Data: Sentz requires users to register with a phone number and email address, and may collect data such as device identifiers and geolocation. Law enforcement agencies may subpoena this information, using it to link transactions to specific users or devices, as well as monitor activity across different jurisdictions
2. Transaction Records and End-to-End Encryption: Sentz transactions are encrypted, but while this encryption protects data from external breaches, transaction metadata (such as timestamps and IP addresses) might still be accessible to Sentz. If legally required, MobileCoin could provide these metadata logs, even if the contents of the transactions remain private.
3. MobileCoin Blockchain Tracking: Sentz operates on the MobileCoin blockchain, where transactions, though private, are traceable in terms of transaction flows without necessarily revealing individual identities. While Sentz uses cryptographic methods to enhance privacy, such as Ring Confidential Transactions (RCTs) and zero-knowledge proofs, these can still be analyzed using blockchain forensic tools, which some agencies use to detect suspicious activity patterns or links to known addresses.
4. eUSD Stablecoin Regulations: Since Sentz transactions utilize eUSD, a stablecoin tied to the value of USD, any compliance requirements for stablecoins could provide additional oversight. Regulatory authorities may work with stablecoin custodians, or even require audits, to track holdings and flows in collaboration with entities like MobileCoin, particularly if suspicious activity is flagged.

Overall, Sentz's combination of streamlined invoicing, fast transaction times, and integration with stablecoins makes it a competitive alternative to services like PayPal and Venmo, especially for users familiar with digital currencies and stablecoin transactions. While Sentz's privacy features and end-to-end encryption make tracking challenging, law enforcement's ability to subpoena data from the company, use blockchain forensics, or enact new stablecoin

regulations could allow some level of monitoring in alignment with regulatory and legal requirements.

ZCash

Zcash (ZEC) is a privacy-focused cryptocurrency that offers two types of addresses: transparent (t-addresses), similar to Bitcoin addresses, and shielded (z-addresses), which provide enhanced privacy features. The privacy features of Zcash make it challenging for law enforcement to track, but several methods and strategies can be employed:

Pros of Zcash for Privacy and Security

1. Optional Privacy with zk-SNARKs:
    - Zcash uses a cryptographic technique called zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), which allows for shielded transactions. These transactions can hide the sender, recipient, and transaction amount, providing a high level of privacy and anonymity.
2. Choice Between Transparent and Shielded Transactions:
    - Users can choose between transparent transactions (which are public and similar to Bitcoin's) and shielded transactions (which are private). This flexibility allows users to maintain privacy when needed and transparency when preferred or required by law.
3. Advanced Cryptography:
    - The use of zk-SNARKs represents a cutting-edge approach to cryptography, providing strong privacy guarantees without requiring a trusted setup beyond the initial "ceremony" that generated the initial parameters.

Cons of Zcash for Privacy and Security

1. Low Adoption of Shielded Transactions:
    - Despite the availability of shielded transactions, many users and exchanges still use the default transparent option. As a result, the privacy benefits of Zcash are not fully realized, and transparent transactions can still be tracked similarly to Bitcoin.
2. Computationally Intensive:
    - Shielded transactions on Zcash require more computational power and time compared to transparent transactions, making them less convenient for everyday use and potentially more costly with a greater environmental impact.
3. Regulatory Scrutiny:

- The strong privacy features of Zcash have attracted regulatory attention and scrutiny in some jurisdictions, which could impact its use and acceptance on regulated exchanges and platforms.

4. Network Privacy Limitations:
    - While all cryptocurrencies offer strong on-chain privacy, it does not inherently protect against network-level privacy threats, such as IP address tracking during transactions. Users may need to employ additional privacy tools (like Tor) to enhance their overall privacy when using any cryptocurrency.

Techniques Used by Law Enforcement to Track Zcash

1. Blockchain Analysis:
    - Transparent Addresses (t-addresses):
        - Transactions involving t-addresses are similar to Bitcoin and are publicly visible on the Zcash blockchain. Law enforcement can use traditional blockchain analysis tools to trace transactions between t-addresses.
    - Shielded Addresses (z-addresses):
        - Transactions involving z-addresses are private, and details such as the sender, receiver, and amount are encrypted. This significantly limits the effectiveness of blockchain analysis for these transactions.
2. Hybrid Transactions:
    - Transactions between t-addresses and z-addresses (and vice versa) create points of transparency that can be exploited. If funds move from a z-address to a t-address, law enforcement can potentially trace the t-address.
3. Intelligence Gathering:
    - Law enforcement can rely on traditional intelligence gathering methods, such as surveillance, informants, and undercover operations, to gather information on individuals using Zcash for illicit activities.
4. Exchange Cooperation:
    - Many Zcash transactions eventually involve cryptocurrency exchanges where ZEC is converted to fiat currency or other cryptocurrencies. Exchanges that comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations can provide user information upon legal request.
5. Network Monitoring:
    - Monitoring the Zcash network traffic can provide some insights, such as IP addresses of nodes participating in transactions. This can help in identifying the geographical locations of users.
6. Targeting Weak Links:
    - Law enforcement can focus on vulnerabilities in the overall ecosystem rather than the Zcash protocol itself. This includes looking for weak links in user behavior, such as poor operational security (OPSEC) practices, that can expose identities.

7. Collaborating with Blockchain Analysis Firms:
    - Some blockchain analysis firms are developing tools to analyze privacy coins, including Zcash. While these tools are not as advanced as those for Bitcoin, they can still provide some insights into Zcash transactions, particularly those involving t-addresses.
8. Legal Pressure on Service Providers:
    - Law enforcement can exert legal pressure on service providers that accept Zcash, such as online marketplaces or payment processors, to gather information on transactions and users.
9. Open-Source Intelligence (OSINT):
    - Investigators can use OSINT techniques to gather information from publicly available sources, such as forums, social media, and other online platforms where individuals may discuss or advertise their use of Zcash.
10. Collaborating with International Agencies:
    - International cooperation can be crucial in tracking Zcash transactions, especially when they cross borders. Law enforcement agencies around the world share information and resources to combat the use of Zcash in illegal activities.

Challenges in Tracking Zcash

1. Enhanced Privacy Features:
    - Zcash's privacy features, particularly those involving shielded addresses, make it difficult to link transactions to individuals or trace the flow of funds.
2. Selective Transparency:
    - The ability to choose between transparent and shielded transactions means that only some parts of the transaction history may be visible, complicating the analysis.
3. Evolving Privacy Techniques:
    - As Zcash continues to evolve, its privacy techniques are continuously improved, making it increasingly challenging for law enforcement to develop effective tracking methods.

Tracking Zcash is challenging for law enforcement due to its strong privacy features, particularly those involving shielded addresses. While traditional blockchain analysis methods are more effective for transactions involving transparent addresses, a combination of intelligence gathering, cooperation with exchanges, network monitoring, targeting weak links, and using advanced de-anonymization techniques can still provide some avenues for investigation. However, the effectiveness of these methods is generally limited compared to cryptocurrencies with less emphasis on privacy.

Non-Crypto Digital Payment Methods Analysis:

In the realm of social justice, where mutual aid funds play a crucial role in supporting marginalized communities, maintaining financial privacy and security for both donors and recipients is essential. For some of these transactions cryptocurrencies may not be the right choice, depending on your personal threat model. We want you to be aware that with these non-crypto options deplatforming, debanking, or other suspension of services can be more likely than cryptocurrencies. As an example, one can fairly easily have their CashApp account shut down for being a part of a bail fund that CashApp considers too risky. That being said, these options are much more user friendly than most cryptocurrencies.

Tools like Apple's W3C Tap-to-Cash, CashApp, prepaid gift cards, USPS Money Orders, and Privacy.com cards offer varying levels of privacy and security to safeguard financial transactions. Apple's W3C Tap-to-Cash and Privacy.com cards protect sensitive data through anonymized, encrypted methods, allowing individuals to contribute discreetly. CashApp offers flexibility, though with limited anonymity, while prepaid gift cards and USPS Money Orders provide a high degree of privacy for users who prefer not to disclose personal banking information. These tools empower (some more, some less) users to engage in safer acts of solidarity, enabling financial support with various degrees of exposed personal data, thus aligning with the broader goals of privacy and equity in the fight for social justice.

Apple Tap-to-Cash

Apple introduced Tap-to-Cash in iOS 18 to allow users to transfer money without sharing any personal information. Two iPhones must come into close contact with one another for the transaction to proceed, as it functions only over Bluetooth, and consequently, there is no buyer protection. Tap-to-Cash requires an Apple Cash account and therefore has many of the same privacy concerns. But Tap-to-Cash is different from the Apple Cash feature in iMessage, which allows users to send cash to people one knows and trusts through iMessage. Unlike Tap-to-Cash, Apple Cash transactions in iMessage are not anonymous, as they rely on verified identities. Since the Tap-to-Cash service launched, the terms and conditions have shifted significantly. As of October 2, 2024, receiving peer-to-peer transactions requires identity verification after $500 is received. While sending funds does not explicitly require identity verification, topping up your account does, making it effectively impossible to send funds without verifying your identity. Apple explains that this requirement ensures Apple Cash balances can be FDIC insured, as they must know the customer's name to insure the funds. This is indeed an FDIC mandate. However, this does not necessarily mean personal information is transmitted during peer-to-peer transactions. Although identity verification is required to load funds, when two iPhones come into proximity for a transaction, the only data exchanged is a user-set username, a timestamp, and the transaction amount.

Tap to Cash does not require sharing any personal information with the person receiving funds; the only identifiable element shared is a user-set username, which is stored locally on the recipient's device but never collected or shared with Apple. And transaction history isn't shared with Apple though it is possible Apple or a dedicated law enforcement team could reconstruct it with data possessed by Apple. This makes Tap to Cash more akin to exchanging physical cash in person.

Tap-to-Cash balances are secured the same way your iphone is secured, using biometric authentication, typically a faceprint or fingerprint. Online transactions are secured using Apple's implementation of the W3C WebAuthn standard. This is part of Apple's broader implementation of web authentication standards aimed at enhancing security and privacy during online transactions and logins. WebAuthn, or Web Authentication, is a web standard developed by the World Wide Web Consortium (W3C) and the FIDO Alliance that allows users to authenticate their identities using secure methods like biometric data or hardware security keys. Apple has integrated WebAuthn into its ecosystem to support secure and privacy-focused authentication.

Tap-to-Cash is still very new, and it will remain to be seen if the privacy claims Apple has made will hold true in real world scenarios.

Pros of Apple's Tap-to-Cash for Financial Transactions:

Privacy:

1. Reduced Exposure of Personal Data:
    - Biometric Authentication: Apple devices often use on-device biometric authentication (Face ID, Touch ID) for WebAuthn, which means sensitive information like passwords or PINs are not transmitted to the server, reducing the risk of exposure.
    - Minimal Data Transmission: WebAuthn uses cryptographic keys for authentication, which minimizes the amount of personal data transmitted during the login or transaction process.
2. User Control:
    - User Consent: Authentication through WebAuthn typically requires user consent, ensuring that the user is actively involved in the authentication process.
3. No Password Storage:
    - Eliminates Passwords: By using biometric data or hardware tokens, WebAuthn reduces the need for storing passwords, which can be a vulnerability if compromised.

Security:

1. Strong Authentication:

   - Public Key Cryptography: WebAuthn uses public key cryptography, which provides a high level of security against phishing attacks and credential theft.
   - Resistance to Phishing: Since authentication relies on cryptographic keys rather than passwords, WebAuthn is highly resistant to phishing attacks that trick users into revealing their credentials.
2. Two-Factor Authentication (2FA):
   - Enhanced Security: WebAuthn can be used as part of a two-factor authentication setup, providing an additional layer of security beyond just a password.
3. Device-Specific Security:
   - Secure Enclaves: Apple devices with Secure Enclave technology offer hardware-level security for biometric data and cryptographic keys, enhancing protection against unauthorized access.
4. Tamper-Resistant Hardware:
   - Secure Elements: For hardware security keys, WebAuthn benefits from the tamper-resistant nature of these devices, which are designed to prevent unauthorized access and manipulation.

Cons of Apple's WebAuth for Financial Transactions:

Privacy:

1. Device Dependency:
   - Limited to Apple Devices: WebAuthn functionality is dependent on having compatible Apple devices, which may limit privacy protection for users who do not use Apple products.
2. Biometric Data Concerns:
   - Biometric Data Storage: While Apple stores biometric data securely on the device, concerns may arise about the potential for data breaches or misuse of biometric information.
3. Data Collection and Sharing:
   - Service Provider Integration: Some services integrated with WebAuthn may still collect data about authentication patterns or other user activities, which could impact privacy if not handled correctly.
4. Data Collection:
   - Personal Information: Apple Cash is reliant on an Apple account which collects personal information such as your phone number, email address, and potentially other data for account verification and functionality.
   - Transaction History: Your transaction history is stored and can be accessed within the app, which could be a concern for those seeking complete privacy.
5. Limited Anonymity:
   - User Profiles: Although Tap-to-Cash provides some level of anonymity, your transactions and account activities are still associated with your personal profile and can be accessed by the app's support team or law enforcement if required.

Security:

1. Device Security Risks:
    - Device Compromise: If an Apple device is compromised (e.g., via malware or physical theft), there is a risk that the security credentials stored on the device could be exposed.
2. Implementation Variability:
    - Inconsistent Support: The level of support and implementation of WebAuthn may vary between websites and services, potentially leading to inconsistent security and user experience.
3. Complexity for Users:
    - User Understanding: Users may face challenges understanding and effectively using WebAuthn features, particularly if they are not familiar with authentication technologies or if they encounter technical issues.
4. Fallback Mechanisms:
    - Alternate Authentication Methods: While WebAuthn provides strong security, fallback authentication methods (e.g., passwords) might still be used in cases where WebAuthn is not supported or fails, potentially introducing vulnerabilities.

Apple's implementation of WebAuthn offers robust privacy and security benefits for financial transactions by leveraging strong authentication methods and reducing reliance on traditional passwords. The use of biometric data and cryptographic keys enhances security and minimizes the risk of credential theft and phishing attacks. However, users should be aware of potential privacy concerns related to biometric data and the dependency on Apple devices. Additionally, the effectiveness of WebAuthn can be influenced by the consistency of its implementation across different services and the security of the user's device. Overall, WebAuthn represents a significant step forward in enhancing online security and privacy, provided users and service providers effectively manage and support the technology.

CashApp

Cash App, developed by Square, Inc., is a popular mobile payment service that allows users to send and receive money, make purchases, and invest in stocks and Bitcoin. It also offers a Cash Card, which can be used for purchases and ATM withdrawals. Here's a detailed look at the privacy and security pros and cons of using Cash App for financial transactions:

Pros of Cash App:

Privacy:

1. User Control Over Transactions:
    - Discreet Transfers: Cash App allows users to send and receive money without disclosing personal banking information to recipients.

- Cash Tag: Users can set up a unique CashTag (a username) for transactions, which helps protect personal information compared to sharing actual bank account numbers.

2. Anonymity Options:
   - No Need for Physical Bank Details: Transactions through Cash App do not require physical bank details to be shared with other users or merchants.
3. In-App Privacy Settings:
   - Control Over Data Sharing: Users have the ability to control certain privacy settings within the app, such as who can see their activity and who can send them money.

Security:

1. Encryption and Security Features:
   - Data Encryption: Cash App uses encryption to protect data transmitted between your device and their servers.
   - Two-Factor Authentication (2FA): Cash App offers 2FA, adding an extra layer of security to your account and reducing the risk of unauthorized access.
2. Fraud Detection:
   - Monitoring Systems: Cash App has fraud detection systems in place to identify and alert users to suspicious activity or potential fraud.
3. Instant Transactions:
   - Immediate Transfers: Transactions are processed quickly, which can be advantageous for both personal and business transactions.
4. Cash Card and ATM Security:
   - Virtual and Physical Cards: Cash App provides a virtual Cash Card for online purchases and a physical card for in-store purchases and ATM withdrawals, with the ability to lock or unlock the card via the app.

Cons of Cash App:

Privacy:

1. Data Collection:
   - Personal Information: Cash App collects personal information such as your phone number, email address, and potentially other data for account verification and functionality.
   - Transaction History: Your transaction history is stored and can be accessed within the app, which could be a concern for those seeking complete privacy.
2. Limited Anonymity:
   - User Profiles: Although Cash App provides some level of anonymity through Cash Tags, your transactions and account activities are still associated with your

personal profile and can be accessed by the app's support team or law enforcement if required.

3. Records Kept by Cash App:
    - Cash App retains records of a user's identity and transactions, which could be subpoenaed or accessed by law enforcement if necessary.

Security:

1. Risk of Account Compromise:
    - Phishing and Scams: Users may be targeted by phishing scams or fraudulent schemes, leading to potential loss of funds or personal information if they fall victim.
    - Account Security: If a user's device is compromised, their Cash App account could be at risk. Ensuring that you use strong, unique passwords and keep your device secure is essential.
2. Limited Fraud Protection:
    - Dispute Resolution: Cash App's dispute resolution and fraud protection processes may not be as extensive as those provided by traditional banks or credit card companies.
    - No Purchase Protection: Cash App does not offer purchase protection or insurance for transactions, meaning you may have limited recourse if a purchase goes wrong or a product is not delivered.
3. ATM Fees and Limits:
    - Fee Structure: Using the Cash Card at ATMs may incur fees, particularly if you do not use an in-network ATM.
    - Transaction Limits: Cash App imposes certain limits on transactions and withdrawals, which might be restrictive for high-value transactions or frequent users.
4. Regulatory and Support Issues:
    - Regulatory Challenges: As a fintech app, Cash App is subject to regulatory scrutiny and may face challenges related to compliance and financial regulations.
    - Customer Support: Some users report difficulties with customer support, particularly in resolving disputes or recovering lost funds.

Cash App offers robust privacy and security features for mobile financial transactions, including encryption, two-factor authentication, and control over user data. It provides a convenient and relatively private way to manage money and make transactions. However, users should be aware of potential privacy concerns related to data collection and account information, as well as the limitations in fraud protection and customer support. For those who value ease of use and mobile access but are concerned about advanced fraud protection, Cash App can be a useful tool, provided users exercise caution and implement additional security measures.

Prepaid Gift Cards

Prepaid gift cards are often used for financial transactions because they offer unique privacy and security benefits, but they also come with certain drawbacks.

Pros of Prepaid Gift Cards:

1. Anonymity and Privacy:
    - Anonymity: Prepaid gift cards do not require personal information for activation or use, offering a high degree of anonymity. This can be beneficial for those who wish to keep their transactions private.
    - Limited Personal Data Exposure: Since there is no need to link the card to a bank account or provide personal identification, the risk of personal data exposure is minimized.
2. Reduced Risk of Identity Theft:
    - Minimal Information Required: Unlike credit or debit cards, prepaid gift cards do not require sensitive personal information, reducing the risk of identity theft if the card is lost or stolen.
3. Fraud Protection:
    - Limited Value: The value of a prepaid gift card is capped at the amount loaded onto the card. This limits potential losses in case of theft or fraud, unlike credit cards which can have higher credit limits.
4. No Direct Link to Bank Accounts:
    - Reduced Account Exposure: Since prepaid cards are not linked to a bank account, unauthorized transactions do not directly affect the cardholder's bank balance.

Cons of Prepaid Gift Cards:

1. Limited Security Features:
    - Lack of Fraud Protection: Many prepaid gift cards lack the robust fraud protection features of credit and debit cards, such as chargeback rights or fraud monitoring.
    - No PIN or Authentication: Some prepaid cards may not require a PIN or have additional security features, making them easier to use by someone who finds or steals the card.
2. No Recovery Options:
    - Lost or Stolen Cards: If a prepaid gift card is lost or stolen, recovering the balance can be difficult or impossible, especially if the card is not registered with the issuer.
3. Lack of Purchase Protection:

- No Insurance for Purchases: Prepaid gift cards generally do not offer purchase protection or insurance benefits that come with credit cards, such as extended warranties or fraud protection for online transactions.

4. Fees and Expiration:
    - Fees: Some prepaid gift cards come with various fees, such as purchase fees, maintenance fees, or inactivity fees, which can reduce the card's value over time.
    - Expiration Dates: Unlike traditional debit and credit cards, some prepaid gift cards have expiration dates, and any unused balance after expiration may be forfeited.
5. Limited Usability and Acceptance:
    - Not Universally Accepted: Some merchants may not accept prepaid gift cards, especially for certain types of transactions (e.g., car rentals, hotel bookings, or online transactions that require address verification).

Prepaid gift cards offer strong privacy benefits due to their anonymity and reduced exposure of personal information. However, they have significant security drawbacks, such as limited fraud protection and the inability to recover funds if the card is lost or stolen. They are best suited for small, low-risk transactions where privacy is a priority and there is enough time to get a physical card to the recipient. For larger or more secure transactions, traditional payment methods with better protection and recovery options might be more appropriate.

USPS Money Order

USPS Money Orders are a popular alternative to checks and electronic payments for various financial transactions. They are issued by the United States Postal Service and can be used to pay bills, send money, or make purchases. Let's explore the privacy and security pros and cons of using USPS Money Orders for financial transactions.

Pros of USPS Money Orders:

Privacy:

1. Anonymity:
    - No Bank Account Required: You do not need a bank account to purchase or cash a USPS money order, which can help maintain anonymity in financial transactions.
    - Minimal Personal Information: Purchasing a money order requires minimal personal information, offering more privacy compared to checks or electronic payments.
2. Confidentiality of Transactions:
    - No Digital Trail: Unlike electronic transactions that leave a digital footprint, USPS money orders do not create a digital record, which can help keep the transaction details private.

Security:

1. Secured Payment Instrument:
    - Prepaid and Guaranteed Funds: A USPS money order is prepaid, meaning it is guaranteed to have funds available when cashed, reducing the risk of bouncing (as opposed to personal checks).
2. Tracking and Replacement:
    - Trackable: Each USPS money order comes with a unique serial number, allowing the purchaser to track it if it is lost or stolen.
    - Replacement Possibilities: If a money order is lost, stolen, or damaged, it can be replaced or refunded (subject to terms and conditions), adding a layer of security to the transaction.
3. Harder to Forge or Alter:
    - Security Features: USPS money orders have several security features (e.g., watermarks, security threads) that make them difficult to forge or alter, reducing the risk of fraud.
4. In-Person Verification:
    - Physical Verification: Since USPS money orders are often bought and cashed in person, there is an opportunity for a face-to-face identity check, reducing the risk of identity theft and unauthorized use.

Cons of USPS Money Orders:

Privacy:

1. Lack of Complete Anonymity:
    - Purchaser Information: While minimal information is required, the purchaser's information (such as name and address) may still need to be provided and is recorded on the money order, reducing total anonymity. This does NOT mean that the recipient's information is required, other than a valid mailing address.
    - Records Kept by USPS: USPS retains records of money orders, which could be subpoenaed or accessed by law enforcement if necessary.
    - Physical surveillance: The process of purchasing and cashing money orders is manual and may require visiting a post office, which may create physical surveillance records such as video recordings of both purchaser and recipient.

Security:

1. Limited Fraud Protection:
    - Susceptible to Theft or Loss: Money orders can be lost or stolen. Although they can be replaced, the process can be time-consuming and involves a fee.

- Fraudulent Money Orders: Scammers may attempt to pass counterfeit money orders, requiring recipients to verify authenticity, especially for transactions involving strangers or large amounts.

2. Inconvenience and Delays:
    - Manual Processes: The process of purchasing and cashing money orders is manual and may require visiting a post office, leading to inconvenience and potential delays in financial transactions.
    - Replacement Delays: In case of loss or theft, obtaining a replacement money order can take several weeks, which might not be ideal for urgent transactions.
3. Fees:
    - Purchase and Processing Fees: USPS charges a fee to issue a money order. Additional fees may apply if the money order is lost, stolen, or needs to be replaced.
    - International Transactions: For international money orders, fees may be higher, and they may not be universally accepted in all countries.
4. Limited Acceptance and Restrictions:
    - Not Universally Accepted: Some businesses or individuals may not accept money orders, particularly for high-value transactions.
    - Cashing Limits: Certain locations have limits on the amount of money that can be cashed using a money order, requiring multiple transactions for larger amounts.

USPS Money Orders provide a secure and relatively private means of conducting financial transactions, especially when cash or electronic methods are not preferred. They are particularly useful for those who do not have access to traditional banking or wish to avoid leaving a digital trail. However, they have limitations in terms of convenience, fees, and fraud protection, making them less suitable for high-value or frequent transactions. Their use may also create a trail of physical surveillance of both purchaser and recipient. Users should weigh these pros and cons to determine if a USPS money order is the right choice for their specific needs.

Privacy.com Card

Privacy.com offers virtual cards that are designed to enhance privacy and security for online financial transactions. These virtual cards can be used for one-time or recurring purchases and provide features aimed at protecting user information. This section reviews the use case scenario of donating to mutual aid funds that have an online presence, as in, if an organization has a “Donate” button on their website and someone wishes to discreetly send funds, a PrivacyCard would help to mask who donated the funds.

Pros of Privacy.com Cards:

Privacy:

1. Anonymity:
    - Virtual Cards: Privacy.com cards are virtual, meaning they don't require physical mail or a direct link to your personal bank accounts, helping to maintain privacy.
    - Masked Personal Information: When using Privacy.com cards, merchants do not see your actual credit card number, reducing the risk of personal information exposure.
2. Controlled Disclosure:
    - Unique Card Numbers: Each transaction or merchant can be assigned a unique card number, minimizing the risk of data leaks and controlling how much information is shared with different entities.
    - No Need for Personal Bank Details: You do not need to provide your personal bank details to merchants, which helps keep your financial information secure.

Security:

1. Enhanced Fraud Protection:
    - Card Limits: You can set limits on how much can be charged to each virtual card, which reduces the impact if a card number is compromised.
    - Single-Use or Merchant-Specific Cards: By using single-use or merchant-specific virtual cards, you limit the risk of fraud and misuse.
2. Easy Management and Tracking:
    - Control Over Transactions: You can easily manage, freeze, or cancel virtual cards through Privacy.com's platform, offering flexibility and control over your financial transactions.
    - Transaction Monitoring: The platform provides real-time tracking of transactions, allowing users to monitor their spending and identify any unauthorized charges quickly.
3. Data Encryption:
    - Secure Communication: Privacy.com employs encryption and secure communication protocols to protect your data from unauthorized access.
4. Dispute Resolution:
    - Chargeback Support: Privacy.com offers support for disputing transactions, which can be useful if you encounter fraudulent charges or issues with merchants.

Cons of Privacy.com Cards:

Privacy:

1. Limited Anonymity:
    - Account Registration Required: To use Privacy.com, you need to create an account and provide some personal information, which means there is a basic level of data collection and account monitoring.

2. Potential Data Collection:
    - Service Provider Data: Privacy.com itself collects data about your transactions and account activities. While they have privacy measures in place, any data collection may still be a concern for privacy-conscious individuals.

Security:

1. Limited Merchant Acceptance:
    - Not Always Accepted: Some merchants may not accept virtual cards or may have restrictions on their use, which could limit the effectiveness of Privacy.com cards for certain transactions.
2. Dependence on Online Platforms:
    - Internet Access Required: Privacy.com cards are virtual and require online access to manage and use. If you encounter technical issues or lack internet access, it might affect your ability to use the service effectively.
3. Potential Technical Issues:
    - Platform Reliability: As with any online service, there is a potential risk of technical issues, outages, or bugs that could affect the ability to use or manage virtual cards.
4. Risk of Account Compromise:
    - Account Security: If your Privacy.com account is compromised, there could be risks to all associated virtual cards. It's important to use strong, unique passwords and enable any additional security features offered by the platform.

Privacy.com cards provide strong privacy and security features for online financial transactions by offering virtual card numbers, transaction limits, and easy management. They are especially useful for controlling exposure of personal financial information and preventing fraud. However, they may have limitations in merchant acceptance and require a balance between privacy and necessary data collection for account management. Users should consider these factors and evaluate how Privacy.com fits their specific privacy and security needs.

Usability Analysis for Mutual Aid

The following chart maps the Profiling and Surveillance, Cyber Security Considerations, Data Protection Role and Responsibilities, as well as Financial Exclusion Aspects of cryptocurrencies and non-cryptocurrencies for financial transactions. In regards to the usability of these financial tools, we want to demonstrate the use case, pros and cons, as well as feasibility for mutual aid groups, individuals, and organizations.

Profiling and Surveillance

- Profiling refers to the automated processing of personal data to evaluate certain aspects relating to an individual. This can include analyzing or predicting various aspects of a

person's behavior, preferences, interests, economic situation, health, location, movements, reliability, or identity.
    - In the context of making payments or donations to abortion clinics, profiling involves collecting and analyzing transaction data to build detailed profiles of individuals who are engaging in these activities. This information can reveal sensitive aspects of a person's life, such as their health status, reproductive choices, and potentially their political and social beliefs. For example, a transaction to an abortion clinic could be used to infer that an individual is seeking abortion services or supporting reproductive rights, which might be considered sensitive or stigmatizing information.
- Surveillance is the monitoring of behavior, activities, or information for the purpose of information gathering, influencing, managing, or directing. This can be done by states, the private sector, or even civil society, often without the knowledge or consent of the individuals being monitored.
    - In the context of making payments or donations to abortion clinics, surveillance involves tracking and analyzing financial transactions to monitor individuals' behaviors and activities related to reproductive health services. This can include observing where, when, and how individuals are making these payments or donations. The primary concern with surveillance in this context is the potential for it to be used to identify, monitor, and potentially target individuals seeking or supporting abortion services. This could lead to invasions of privacy, stigmatization, harassment, or legal consequences, particularly in states where abortion services are highly regulated or restricted.

Cybersecurity Considerations

- Cybersecurity risks refer to the potential threats and vulnerabilities that can compromise the security, integrity, and confidentiality of digital payment systems. These risks can arise from various sources, including unauthorized access, cyber-attacks, data breaches, and technological advancements that undermine current security protocols.
    - Unauthorized Access and Credential Compromise: Cyber attackers may use techniques such as social engineering, malware, and side-channel attacks to gain access to users' credentials. Unauthorized access could lead to the exposure of sensitive information about individuals seeking or supporting abortion services, potentially resulting in privacy violations, harassment, or legal repercussions.
    - Data Breaches: Concentrated storage of payment data in central databases makes these repositories attractive targets for cyberattacks. A data breach could expose the personal and financial details of individuals making payments or donations to abortion clinics, leading to widespread privacy violations and potential identity theft.
    - Quantum Computing Threats: The advent of quantum computing poses a threat to current encryption methods used to secure digital payments. If quantum

computers compromise existing cryptographic protections, the confidentiality and integrity of transactions to abortion clinics could be at risk, exposing sensitive information.
    - DoS Attacks: Centralized payment systems are vulnerable to DoS attacks, which could disrupt the processing of payments and donations to abortion clinics. Such disruptions could undermine the reliability of digital payment methods and deter individuals from using them.
    - Double-Spending Attacks in Distributed Systems: In distributed payment architectures, ensuring the integrity of transactions is crucial to prevent double-spending attacks, where a digital payment is illegitimately spent multiple times. These attacks could undermine trust in the payment system and result in financial losses.
    - Cross-Jurisdictional Data Transfer Risks: Transferring personal and transaction data across multiple jurisdictions can amplify the scale and speed of potential data breaches, or expose data to more regulatory authorities who can access records. Different regulatory environments may have varying levels of human rights protections, increasing the risk of data access and data exposure.

Data Protection Roles and Responsibilities

- Data protection roles and responsibilities refer to the specific duties and obligations assigned to various actors within a digital payment ecosystem to ensure the secure processing, handling, and storage of personal information. These roles are crucial for maintaining compliance with data protection laws and regulations and financial services laws and regulations.
    - In the context of making payments or donations to abortion clinics, understanding the data protection roles and responsibilities is essential due to the sensitive nature of the data involved. Various actors, including government entities, private intermediaries, and private companies, may participate in processing this data. Recognizing their distinct roles and responsibilities is key to ensuring robust data protection practices, however these can also be commercially sensitive relationships and harder to dissect/identify.

Financial Exclusion

- Financial inclusion refers to the process of ensuring that individuals, groups, and organizations have access to useful and affordable financial products and services that meet their needs. Financial exclusion, on the other hand, describes the lack of access to these financial services. This can be due to systemic barriers, poor design choices, or intentional policies, among other reasons, that prevent certain individuals or groups from participating in the financial system.

    In the context of making payments or donations to abortion clinics…

- Design and Accessibility: Poorly designed systems may exclude people with limited digital skills, unreliable internet access, or those from poor communities and undocumented/migrant backgrounds. Ensuring that the system can be easily used by older adults, youth, individuals with disabilities, and rural populations is essential for promoting financial inclusion.
- Infrastructure and Support: Access to reliable internet and digital devices is a prerequisite for using digital payment systems. Marginalized communities sometimes lack these resources, which can lead to accidental financial exclusion. Additionally, providing social support, such as educational programs (financial literacy training) and customer service, is crucial to help these communities adopt and effectively use digital payment methods.
- Dependence on Existing/Traditional Banking System: Systems that rely heavily on traditional banking infrastructure may not benefit unbanked individuals who distrust banks or are denied access to banking services. For example, a digital payment system fully intermediated by banks is unlikely to increase financial inclusion for these groups, as they likely have the same access constraints.
- Policy and Regulation: Poorly conceived policies around digital payment systems can result in accidental financial exclusion. For instance, eliminating physical cash would likely have a detrimental effect on abortion clinics and their ability to receive anonymous, lawful donations.
- Intentionality: Governments may intentionally exclude certain individuals or groups from using digital payment systems as a form of repression. This exclusion can significantly impact individual rights and freedoms. For example, anti-money laundering and counter-terrorism measures can disproportionately affect minority populations, while more explicit exclusion might target ethnic or religious minorities or immigrants. Systems that allow governments to cut off access to individuals or groups pose higher risks of financial exclusion compared to those that treat transactions as cash-equivalent, and morality-based pursuits may target abortion clinics.

Financial Tools	Profiling and Surveillance	Cybersecurity Considerations	Data Protection Roles and Responsibilities	Financial Exclusion Aspects
Bitcoin *These responses assume a selfheld Bitcoin wallet is being used by both parties; and not a wallet on a centralized*	- Public Ledger: All Bitcoin transactions are recorded on a public blockchain, which is transparent and can be analyzed by anyone. Sophisticated data	- Risk of Hacking and Theft: While the Bitcoin network itself is secure, users' wallets can be hacked if they are not properly secured. The	- User is Solely Responsible for Private Keys: Users are solely responsible for the security of their private keys. If these keys are lost or	- Volatility: Bitcoin's price is highly volatile, which can pose a risk for donors and recipients. The value of a donation could fluctuate

exchange like Coinbase. *Exchanges may be required by local law to implement Know Your Customer (KYC) procedures, which can compromise the anonymity of Bitcoin transactions.* Independent Security Analysis: https://www.egr.msu.edu/~renjian/pubs/Blockchain-IoT.pdf "Bitcoin suffers inherent privacy issues in that attackers could link certain identities to their pseudonyms (such as Bitcoin addresses) and identify their history of transactions. This is known as the linking problem. Many users publish their real identities and Bitcoin addresses online so that others can make payments to them. This practice is common among blogs and Websites that request BTC as donations or those selling a product or service. These actions could jeopardize their anonymity. Another common example is	analysis techniques, such as blockchain analysis, can de-anonymize users by linking transactions to real-world identities, especially if combined with data from other sources. + Pseudonymity: Bitcoin transactions are pseudonymous, meaning they are not directly tied to personal identity unless voluntarily linked by the user. This can provide a layer of privacy for individuals making sensitive transactions, such as contributions to mutual aid initiatives. No Central Authority: Bitcoin is decentralized, meaning there is no central authority that collects all transaction data. This decentralization reduces the risk of surveillance by a single organization, offering greater privacy protection in mutual aid scenarios.	loss of private keys, for instance, results in the permanent loss of funds. Irreversible Transactions: Bitcoin transactions are irreversible. If a user accidentally sends Bitcoin to the wrong address or is scammed, there is no recourse to reverse the transaction, which could be a significant consumer protection risk. However, this feature also means that transactions cannot be frozen or reversed by authorities, offering security for mutual aid efforts in sensitive contexts. + Strong Cryptographic Security: Bitcoin transactions are secured by strong cryptographic protocols, making them resistant to tampering and fraud. The decentralized nature of Bitcoin reduces the risk of centralized failures, ensuring that once a Bitcoin wallet receives funds, the transaction is secure and cannot be reversed.	mishandled, it can lead to permanent loss of funds and potential exposure of transaction data. + No Central Data Repository: There is no centralized repository of personal data in Bitcoin transactions, which reduces the risk of reidentification. With careful management, users can maintain a high level of privacy when making payments, which is crucial for mutual aid activities that require discretion.	significantly, leading to uncertainty and potential financial loss. Technical Barriers: The use of Bitcoin requires a certain level of technical knowledge, which might exclude individuals who are less tech-savvy, such as older adults or those in regions with limited access to technology. + Accessibility: Bitcoin can be sent and received anywhere in the world without the need for a bank account, making it accessible to people in regions with limited banking infrastructure. However, converting Bitcoin to fiat currency requires use of a third party exchange service, which may necessitate a bank account and identity verification, potentially limiting accessibility for some users.

when users trade BTC for other altcoins over exchange platforms. Most exchange platforms require users to validate their identities by uploading a copy of official identification, which exposes the users to the exchange applications. Such examples do not require an attacker to learn the full transaction history of those users. Simply by tracing the Bitcoin addresses over the blockchain, the transactions could be revealed. In fact, even cautious users who do not publicly use their identities may be at risk as well."				
Monero Independent Security Analysis: https://www.comp.nus.edu.sg/~prateeks/papers/Monero-analysis.pdf "Our results show that in 88% of cases, the origin of the funds can be easily determined with certainty."	- Difficult to trade without risk: Because its transactions are known for being difficult to track, legitimate exchanges do not wish to accept this cryptocurrency, pushing users towards sketchier exchanges and ghost websites. + No Public Ledger Traceability: Unlike	- Vulnerabilities to Local Attacks: Malware, phishing, and other forms of cyberattacks could compromise a user's private keys, leading to the loss of funds. Because Monero transactions are irreversible, recovering stolen funds is nearly impossible, making the consequences of	- User Responsibility: As with other cryptocurrencies, the security of Monero is only as strong as the user's own practices. If users do not properly secure their private keys or wallets, they could still be vulnerable to hacks or theft, despite the inherent security of the Monero network.	- Deflationary: Monero, like other cryptocurrencies, has a fixed supply, which makes it deflationary over time. This characteristic can potentially increase the value of Monero holdings as demand grows, but it also means that the currency may not be as liquid or easily traded as more

	Bitcoin, where all transactions are recorded on a transparent public ledger, Monero's blockchain is obfuscated. This means that the amounts, origins, and destinations of transactions are hidden, providing a higher level of privacy and reducing the risk of profiling by third parties. Strong Privacy Features: Monero is specifically designed to enhance privacy through technologies like Ring Signatures, Ring Confidential Transactions, and Stealth Addresses. These features obscure the details of transactions, making it extremely difficult for third parties to trace payments or link transactions to specific individuals, which is particularly useful in maintaining the confidentiality of mutual aid activities.	such attacks severe. + Community-Driven Security: Monero is supported by a community of developers who work to improve the security and privacy features of the network. Regular updates help the protocol stay ahead of emerging threats and vulnerabilities.	+ Decentralized Control: Monero operates on a decentralized network with no central authority managing or storing data. This decentralization reduces the risk of large-scale data breaches or misuse of personal information by centralized entities, as no single entity has control over the network. Users are therefore protected from the vulnerabilities associated with central data repositories.	widely accepted cryptocurrencies. Illiquid: Because legitimate exchanges do not wish to accept this cryptocurrency, it is difficult to convert into fiat currency. When it is accepted, users often face high fees. Additionally, the need to use less reputable exchanges to trade Monero increases the risk of encountering scams or fraudulent platforms, where funds may not be returned. +
MobileCoin, specifically its integration with Signal Independent Security Analysis: A partial answer can	- Public Blockchain Data: Even though Signal adds a layer of privacy, MobileCoin transactions are still recorded on a blockchain. While details are obfuscated,	- Relatively New and Untested: As a newer cryptocurrency, MobileCoin has not been as extensively tested in the wild as older cryptocurrencies like	- Lack of Centralized Support: The decentralized and privacy-focused nature of MobileCoin means there is limited centralized support or recourse in case of	- Limited Acceptance: As a relatively new and specialized cryptocurrency, MobileCoin is not widely accepted, including by reputable exchanges.

be found in this paper, which explores the known weaknesses in the Stellar Consensus Protocol, on which MobileCoin was built: https://arxiv.org/pdf/1904.13302	the public nature of the blockchain means that advanced techniques could potentially be used to analyze and infer certain patterns, particularly if combined with other data sources. + Signal Integration for Discussions About the Transaction: MobileCoin's integration with Signal allows users to send and receive MobileCoin directly within the Signal app, which has end-to-end encryption. This integration ensures that communication about the transaction is fully encrypted.	Bitcoin. This could mean there are undiscovered vulnerabilities that could be exploited by attackers. Dependence on Mobile Device Security: The security of MobileCoin transactions depends heavily on the security of the user's mobile device. If the device is compromised, the user's MobileCoin wallet could be at risk, potentially leading to theft or unauthorized transactions. + Mobile-First Security Design: MobileCoin is designed specifically for mobile devices, with a focus on security and ease of use. This design helps protect users from many common mobile security threats, such as SIM swapping or malware attacks on smartphones.	lost funds or security issues. Users have to manage their own security and data protection. + Minimal Data Collection: MobileCoin and Signal together collect minimal data, adhering to privacy-focused principles. This reduces the risk of data breaches or misuse by third parties. User-Controlled Privacy: MobileCoin, especially when integrated with Signal, gives users control over their transaction data. The decentralized nature of the system means users are responsible for their own privacy, reducing reliance on third parties to protect personal information.	This could limit its usefulness for individuals needing to convert it to fiat currency or use it in environments where only more widely accepted payment methods are available. + Accessible via Mobile Devices: MobileCoin's mobile-first design makes it potentially more accessible to individuals who primarily use smartphones. Users can cash MobileCoin out to their bank account in-app, similar to Cash App. Low Technical Barrier for Mobile Users: MobileCoin's native app and integration into Signal makes it relatively easy to use, which can be a significant advantage for users with varying levels of technical expertise.
ZCash Independent Security Analysis: Note, this analysis was funded by	- Public Transactions: Zcash transactions are not private by default. If users opt for or mistakenly use transparent	- Complexity in Use: The use of shielded transactions requires a certain level of technical understanding. Users	- Responsibility on the User: As with other decentralized cryptocurrencies, the responsibility for data protection lies	- +

Zcash, but it was published and conducted independently by the NCC Group. https://research.nccgroup.com/wp-content/uploads/2023/10/NCC_Group_ZcashFoundation_E008263_Report_2023-10-20_v1.1-1.pdf	transactions (which are similar to Bitcoin transactions), the transaction details will be visible on the public blockchain, exposing them to potential profiling and surveillance. + Shielded Transactions: Zcash offers the option of using shielded transactions, which are fully private and encrypted. This means that the details of the transaction (such as the sender, receiver, and amount) are not visible on the public blockchain, significantly reducing the risk of profiling and surveillance.	who are unfamiliar with the process may accidentally send transactions through the transparent layer, compromising their privacy. Wallet Vulnerabilities: While the Zcash network is secure, the security of funds depends on the wallet used. If a wallet is compromised due to poor security practices, the user's funds and privacy could be at risk. +	primarily with the user. Mismanagement of private keys or failure to use shielded transactions correctly can lead to unintended exposure of sensitive information. + User-Controlled Privacy: Zcash gives users control over the privacy of their transactions. By choosing shielded transactions, users can ensure that their transaction data is not exposed to third parties, minimizing the risk of data breaches.	
CARD.com Prepaid Card	- Potential Reporting to Authorities: Financial transactions with prepaid cards are subject to regulatory oversight in certain situations, these transactions could be flagged as suspicious and potentially reported to authorities, particularly if they involve donations or funding to (or perceived to be funding) politically sensitive causes, which may include causes	- Less Protection Compared to Credit Cards: Prepaid cards typically offer fewer protections compared to credit cards, such as chargeback rights, which can leave users more vulnerable if they fall victim to a scam. + Control Over Spending: Prepaid cards limit spending	- Potential Data Sharing with Third Parties: CARD.com may share user data with third-party entities for various purposes, including marketing (with the opt-in of a user), fraud prevention, and regulatory compliance. This sharing could expose users to potential privacy risks, especially if third parties do not uphold the same level of	- Fees: Prepaid cards come with various fees, such as card issuance charges. These can make the card less cost-effective for low-income users, potentially leading to financial strain. Dependence on Reloading: Users must continuously reload the card to keep it functional, which can be inconvenient.

	supported by mutual aid groups. + Limited/No Account Sharing: As a prepaid card, it does not have to be directly linked to a bank account. This can offer a degree of separation between one's primary financial accounts and the transactions you make with the card, reducing the risk of direct profiling and identification.	to the amount loaded on the card. This feature can help mitigate the financial impact if the card is compromised, as potential losses are capped at the card's balance.	data protection. + Anonymity, if Desired, from the Merchant: It is not mandatory to provide a merchant with one's real name or address, and CARD.com does not validate these fields. Therefore, while CARD.com will know where money is spent, the entity processing a card number does not need to know who the owner of the card really is.	+ Accessibility: Prepaid cards are accessible to a wide range of users, including those without bank accounts or those with poor credit histories. This inclusivity makes it a viable financial tool for individuals who might otherwise be excluded from other financial services. Ease of Use: The card can be easily obtained and loaded with cash.
USPS Money Order	- Potential for Surveillance at Point of Purchase: If buying a money order in-person, surveillance cameras or other monitoring methods at postal offices might still capture identifying information about the buyer. This is, however, less likely to be as invasive as digital profiling. In addition, if paying for the money order with a credit card instead of cash, it could be traced in this manner. +	- None identified + Offline Transactions: As a non-digital payment method, USPS money orders are not susceptible to cyber-attacks like hacking, phishing, or malware. This significantly reduces the risk of financial data breaches.	- None identified + Federal Oversight: Being a government entity, USPS is subject to federal regulations regarding privacy and data protection (while the US does not have a federal data protection law covering the private sector, it does have a federal privacy law covering government agencies), providing an additional layer of oversight and accountability.	- Physical Access Required: Individuals must physically go to a post office to purchase a money order, which could be a barrier for those with limited mobility or those living in remote areas without easy access to postal services. However, post offices have good geographic breadth, so most people can get to a post office. Price: Money orders are free to redeem, but not free to purchase. A money

	Anonymity for Purchaser: USPS money orders offer a higher degree of anonymity compared to digital payment methods. The purchase of a money order requires no personal information, especially if paid in cash, and the transaction is less likely to be tracked back to the individual donor or payer. Anonymity for Redeemer: USPS does require photo ID to redeem a money order if it has been made out to a name, but if made out to 'cash' no ID is required to redeem it. Even if made out to a name, this information is not digitized and ID is visually sighted but not copied/stored. Lack of Digital Footprint: Since USPS money orders are a paper-based method, they leave no digital trail that can be easily analyzed for profiling purposes. This greatly reduces the risk of personal data being collected and used to infer sensitive information.			order in the amount of less than $500 costs $1.25. A money order for $501 - $1,000 costs $1.75. Maximum Value: The maximum value of a money order is $1,000. However one can purchase multiple money orders. + Accessibility: USPS money orders can be purchased at any post office with cash, making them accessible to individuals without bank accounts or credit cards. This inclusivity is beneficial for those who may not have access to traditional banking services.
Privacy.com Card	- Merchant-Locked	- Potential for	- Data Visibility to	- Disposable/Free

	Cards Privacy.com creates single-use or merchant-locked cards, which means transactions can be limited to specific contexts. This means that Privacy.com is actively filtering out different transactions. Indeed their terms of service states, "You may not use the Services for the following businesses or activities in the following industries … (9) high-risk products and services … , or (10) any industry that exposes you, other Privacy users, our partners, or Privacy to possible harm." This broad language is open to interpretation, potentially limiting the ability to support politically sensitive causes through their services. Limited Anonymity Among Privacy.com While Privacy.com aims to protect users' personal and payment information from merchants and fraudsters, it does add another layer where transaction data is aggregated. Privacy.com itself becomes an additional entity with access to this data. According to	Credential Theft: Users are vulnerable to sophisticated cyberattacks, like social engineering or malware, that target credentials directly on their devices. If credentials are compromised, it could expose their transaction history, potentially revealing their involvement in funding politically sensitive causes. + New Card Numbers: Virtual cards can be easily paused, closed, or set to single-use. This feature significantly reduces the risk of data breaches from third parties. By using a new virtual card for each transaction, users can mitigate the risk of their transactions being pooled to re-identify the person who made a payment.	Identity Verification Provider: Privacy.com requires users to provide a government ID for identity verification, which is handled by a third-party service, Onfido. The ID data is stored by Onfido for at least 30 days to meet Know Your Customer (KYC) requirements. While KYC compliance is legally necessary, outsourcing this process to a third party introduces additional privacy risks. Linked to a Bank Account: While not required, the most prominent (and recommended) way to fund an account is by connecting Privacy.com to a bank account with Plaid. Plaid's privacy policy indicates that it collects comprehensive transaction data, which can be used for advertising and other purposes. This linkage could expose users' financial activities to third-party analysis, increasing the risk of profiling and reducing the anonymity that users might seek when	Email Addresses Not Supported: Privacy.com does not allow account creation linked to anonymous email addresses or common free email services (i.e. Yandex). This restriction could be a barrier for users seeking to maintain anonymity while participating in politically sensitive mutual aid activities. + Permitted Use of Fake Name/Address: When making purchases using a Privacy.com card, it is permitted to use a fake name/address if the merchant requests this information. Privacy.com explicitly says they will not validate this data.

	their Terms of Service, users authorize Privacy.com to share information about their accounts and transactions with law enforcement if necessary. This may reduce the overall privacy for users, especially when supporting politically sensitive causes. + Merchants Can't Identify Who Made a Payment Privacy.com generates virtual card numbers, masking the user's actual financial details. This reduces the ability of third parties to track and profile individuals based on their transaction data In the context of mutual aid, this is beneficial as it ensures that merchants cannot necessarily identify the individuals making payments, thereby protecting the privacy of those supporting sensitive causes.		funding politically sensitive causes through mutual aid initiatives.	

Future Concerns

The future of cryptocurrencies is shaped by a complex interplay of technological, regulatory, and social factors. Balancing privacy, security, and compliance will be a key challenge as the cryptocurrency landscape evolves. Staying informed and proactive in addressing these concerns is crucial for individuals and organizations involved in the cryptocurrency ecosystem.

It is essential to stay informed and proactive in addressing emerging risks and regulatory changes. Balancing innovation, privacy, security, and compliance will remain a key challenge for stakeholders in the cryptocurrency ecosystem.

1. Regulatory Changes and Compliance

- KYC and AML Requirements: Governments may impose stricter Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, potentially eroding privacy.
- Central Bank Digital Currencies (CBDCs): The rise of CBDCs could lead to increased surveillance and control by central authorities, impacting the privacy that traditional cryptocurrencies provide.
- EU bans anonymous crypto payments to hosted wallets

2. Transaction Traceability

- Blockchain Analysis Tools: Enhanced blockchain analysis tools can deanonymize users by linking transactions to real-world identities. Companies and governments use these tools to track and monitor activities.
- Data Leakage: Metadata and patterns in transactions can inadvertently reveal user identities and financial behavior.

3. Quantum Computing

- Cryptographic Vulnerabilities: Quantum computers could break the cryptographic algorithms that secure blockchain transactions, leading to potential breaches in the security of cryptocurrency systems.
- Race for Quantum-Resistant Algorithms: The development and adoption of quantum-resistant cryptographic algorithms are critical to ensure future security.
- For more read: Harvest now, decrypt later

4. Smart Contract Security

- Vulnerabilities and Exploits: Smart contracts are prone to coding errors and vulnerabilities, leading to potential exploits and loss of funds.
- Audit and Verification Challenges: Ensuring the security and correctness of smart contracts is a complex and evolving challenge that requires robust auditing and verification methods.
- How a 27-Year-Old Codebreaker Busted the Myth of Bitcoin's Anonymity

5. Privacy Enhancements

- Private Transactions vs. Regulatory Compliance: Innovations in privacy-preserving technologies, like zk-SNARKs or MimbleWimble, may conflict with regulatory demands for transparency.

- Balancing Privacy and Transparency: The ongoing debate on how to balance user privacy with the need for transparency and compliance in financial systems.

6. Cybersecurity Threats

- Phishing and Social Engineering: Users remain vulnerable to phishing attacks and social engineering tactics that aim to steal private keys and access credentials.
- Hacks and Attacks on Exchanges: Cryptocurrency exchanges are frequent targets of hacking attempts, leading to significant losses for users.

7. Decentralized Finance (DeFi) Risks

- Liquidity and Smart Contract Risks: DeFi platforms introduce new risks related to liquidity, smart contract vulnerabilities, and governance issues.
- Interoperability and Composability Risks: The interconnected nature of DeFi protocols can lead to cascading failures and systemic risks.

8. Governance and Control

- Centralization of Mining and Nodes: Concentration of mining power and control over network nodes can undermine the decentralization and security of blockchain networks.
- Protocol Governance Risks: Disputes over protocol upgrades and governance decisions can lead to forks and instability in the network.
- Funder Control: Venture Capitalist (VC) who fund many of these cryptocurrency companies often have control over the organization itself, thus the organization has a fiduciary responsibility to their funders.
- Funding Runway: As with all VC backed companies, they are beholden to financial constraints of their investors.

9. User Education and Awareness

- Complexity and Usability: The complexity of cryptocurrency systems can lead to user errors and security vulnerabilities.
- Lack of Awareness: Users may not be fully aware of the risks and best practices for securing their assets, leading to potential losses.

10. Environmental Impact and Sustainability

- Energy Consumption: The high energy consumption of proof-of-work cryptocurrencies raises concerns about their long-term sustainability and environmental impact.
- Shift to Sustainable Models: The transition to more energy-efficient consensus mechanisms, like proof-of-stake, introduces new security and governance challenges.

11. Global Political and Economic Dynamics

- Geopolitical Risks: Cryptocurrencies may become entangled in geopolitical conflicts and economic sanctions, affecting their stability and usability.
- Economic Instability: The adoption of cryptocurrencies in unstable economies can lead to increased volatility and regulatory crackdowns.

Emerging Risks

1. Decentralized Autonomous Organizations (DAOs) Vulnerabilities
    - Governance Manipulation: DAOs can be susceptible to governance attacks where a small group of stakeholders manipulates voting to their advantage.
    - Smart Contract Failures: As DAOs rely heavily on smart contracts, any flaw can have severe consequences, leading to loss of funds or system failures.
2. Cross-Chain Interoperability Issues
    - Bridge Vulnerabilities: Cross-chain bridges, used to facilitate transactions between different blockchains, are potential weak points that can be exploited by attackers.
    - Protocol Compatibility Risks: Differences in blockchain protocols can create security and operational challenges, potentially leading to asset loss or transaction failures.
3. Privacy Coins and Their Implications
    - Legal Restrictions: Increased scrutiny of privacy-focused coins (like Monero or Zcash) could lead to bans or restrictions in various jurisdictions.
    - Evasion of Regulations: Privacy coins might be used to bypass regulations, posing risks of illegal activities and making them targets for regulatory crackdowns.
    - Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies
4. Decentralized Finance (DeFi) Innovations
    - Algorithmic Stablecoin Risks: Failures of algorithmic stablecoins, as seen in previous cases (e.g., TerraUSD), highlight the risk of innovative financial products without proven stability mechanisms.
    - Complex Derivatives and Financial Instruments: The rise of complex derivatives and synthetic assets in DeFi could lead to systemic risks and unforeseen financial instabilities.
5. Social Engineering and Phishing Attacks
    - Increasing Sophistication: Attackers are developing more sophisticated methods to trick users into revealing private keys or other sensitive information.
    - Exploitation of Human Behavior: As technology advances, social engineering attacks increasingly exploit psychological and behavioral vulnerabilities.
6. Decentralized Identity (DID) Systems
    - Data Security Risks: Decentralized identity systems can introduce risks related to the security of identity data and the potential for unauthorized access.

    - Interoperability Challenges: Ensuring seamless integration and compatibility between different DID systems poses technical and security challenges.
7. Scalability and Performance Issues
    - Network Congestion and High Fees: Popular networks can experience congestion and high transaction fees, leading to decreased usability and increased security risks.
    - Layer 2 Solutions Vulnerabilities: Layer 2 scaling solutions, while addressing some scalability issues, may introduce new vulnerabilities and attack vectors.
8. Cryptocurrency Custody and Insurance
    - Lack of Standardized Insurance: The absence of standardized insurance solutions for cryptocurrency assets poses significant risks for both retail and institutional investors.
    - Custodial Risks: Entrusting third parties with asset custody introduces counterparty risks and potential for mismanagement or fraud.

Regulatory Changes

1. Global Coordination and Harmonization of Regulations
    - International Collaboration: Regulatory bodies are increasingly collaborating to develop coordinated frameworks for cryptocurrency regulation, aiming to address cross-border challenges.
    - Standardization of Compliance Requirements: Efforts to standardize compliance requirements across jurisdictions could impact how cryptocurrencies are used and traded globally.
2. Increased Focus on Environmental Impact
    - Sustainability Regulations: Regulations targeting the environmental impact of cryptocurrency mining, especially proof-of-work networks, are gaining traction. This could lead to restrictions or incentives for greener practices.
    - Mandatory Environmental Reporting: Regulators may require companies involved in cryptocurrency to report their environmental impact and implement sustainability measures.
3. Consumer Protection and Market Stability Measures
    - Enhanced Disclosure Requirements: Regulators may impose stricter disclosure requirements on cryptocurrency projects and exchanges to protect consumers and investors.
    - Market Manipulation and Fraud Prevention: Increased regulatory focus on preventing market manipulation and fraudulent activities in the cryptocurrency space could lead to stricter enforcement actions.
4. Taxation and Reporting Obligations
    - Automated Tax Reporting: Governments are exploring ways to automate tax reporting for cryptocurrency transactions, potentially impacting privacy and operational processes.

- Global Tax Treaties and Agreements: International agreements on taxation of digital assets could lead to more comprehensive and coordinated tax policies.

5. Cybersecurity Standards and Requirements
    - Mandatory Cybersecurity Measures: Regulatory bodies may introduce mandatory cybersecurity standards and requirements for cryptocurrency exchanges, wallets, and platforms.
    - Incident Reporting and Response Protocols: Enhanced requirements for incident reporting and response protocols aim to improve transparency and accountability in the event of security breaches.
6. Legal Status and Recognition of Cryptocurrencies
    - Clarification of Legal Definitions: Ongoing efforts to clarify the legal status and definitions of cryptocurrencies and related assets could impact their treatment under existing laws.
    - Recognition of Smart Contracts and DAOs: Legal recognition and regulation of smart contracts and DAOs could influence their development and adoption.
7. Regulation of Decentralized Finance (DeFi)
    - Frameworks for DeFi Regulation: Regulatory bodies are exploring frameworks for regulating DeFi platforms and services, balancing innovation with consumer protection and risk management.
    - Licensing and Registration Requirements: DeFi platforms may face licensing and registration requirements similar to traditional financial institutions.